

Implante o Cisco Secure Endpoint/Secure Client usando o Microsoft Intune

Contents

Introdução

Este documento descreve o processo para implantar o Cisco Secure Endpoint ou Secure Client usando o Microsoft Intune. O documento mostra as etapas de como criar um aplicativo suportado pelo Microsoft Intune a partir dos instaladores do Secure Endpoint/Secure Client e, em seguida, usa isso para implantação usando o centro de administração do Microsoft Intune.

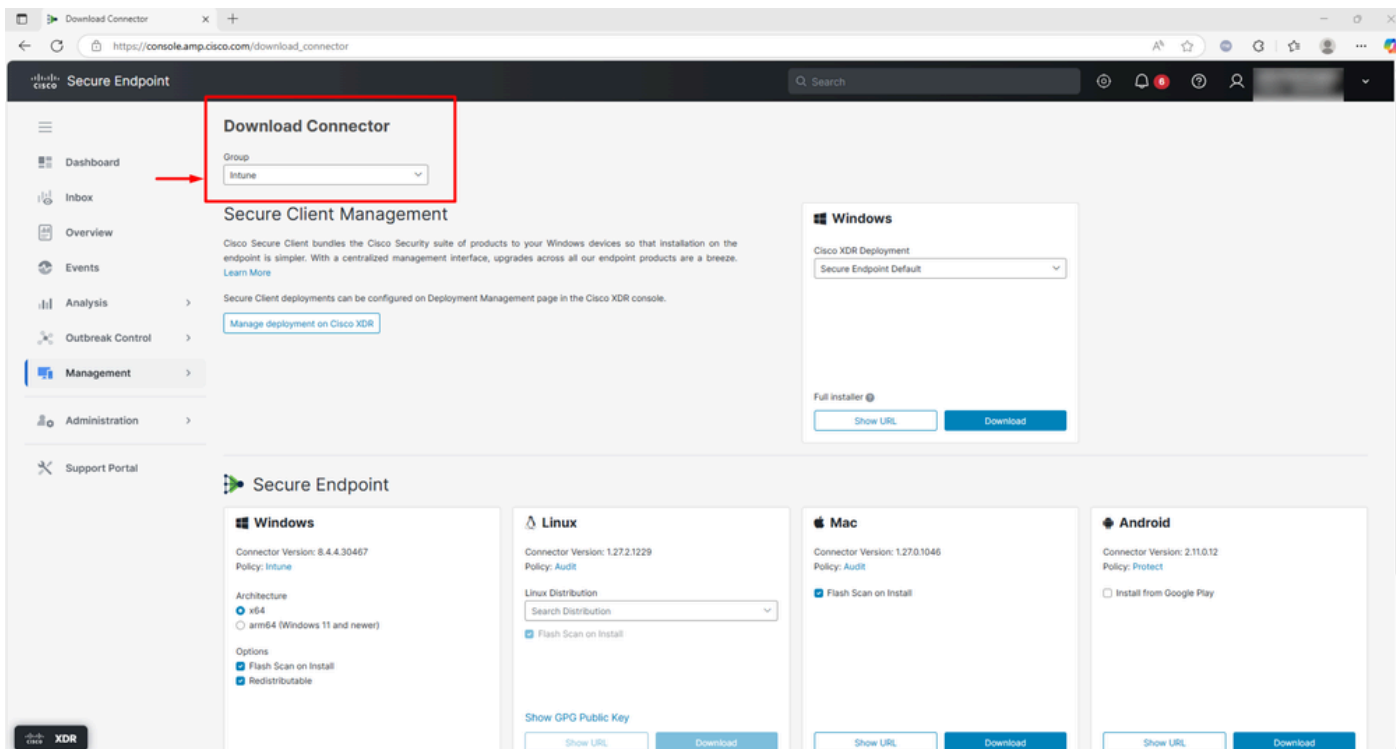
Especificamente, o processo inclui o empacotamento do instalador do Cisco Secure Endpoint como um aplicativo Win32 usando a Ferramenta de Preparação de Conteúdo Intune Win32, seguido pela configuração e implantação do aplicativo por meio do Intune. Usamos a ferramenta oficial Microsoft Prep para criar o aplicativo.

Configuração

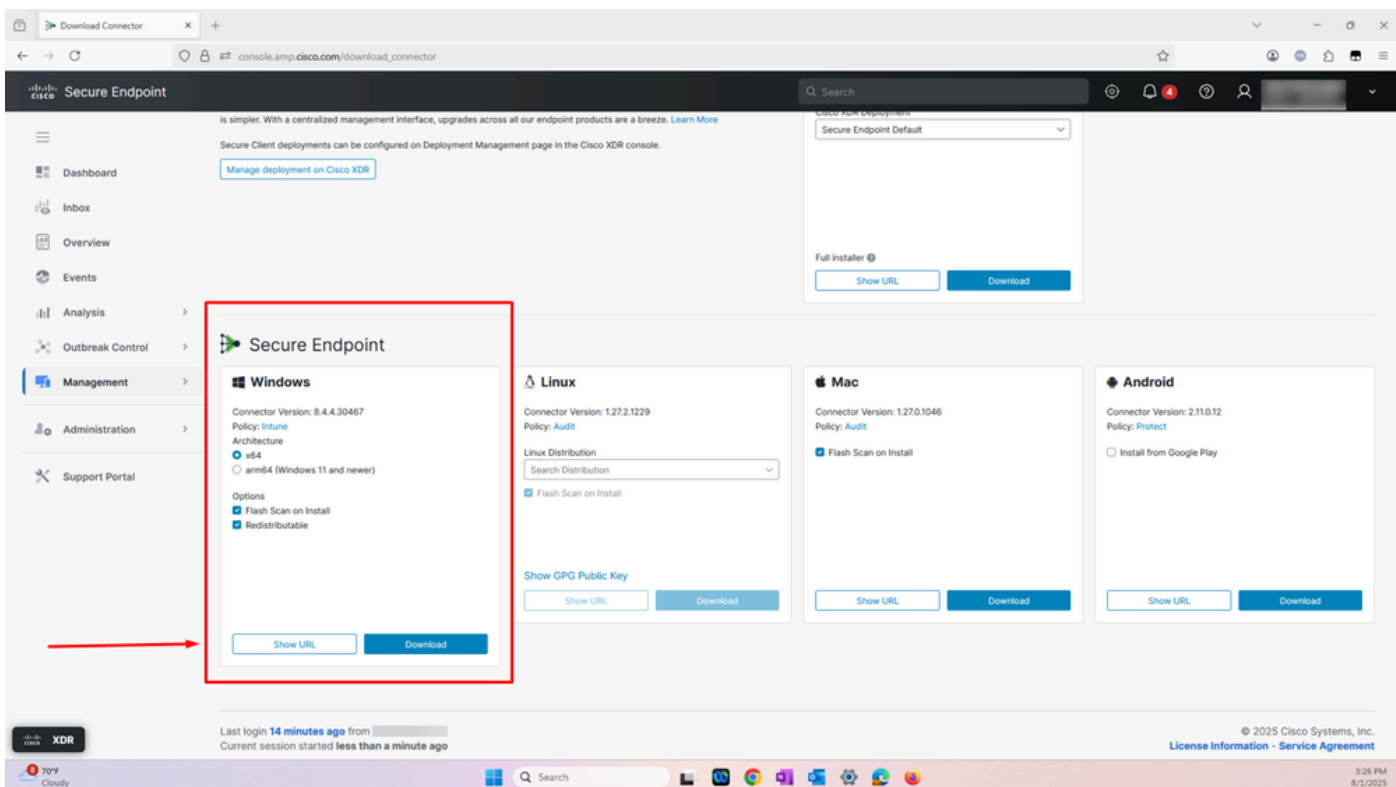
Implantação segura de endpoint

Etapa 1. Faça o download do Cisco Secure Endpoint Installer.

- Faça login em seu respectivo Secure Endpoint Portal, dependendo da região:
<https://apps.security.cisco.com/overview>
- Navegue até a guia Management e selecione Download Connector
- Selecione o grupo de Pontos de Extremidade Seguros no qual você deseja que o conector se registre



- Selecione download e o instalador EXE será baixado localmente, como mostrado na captura de tela



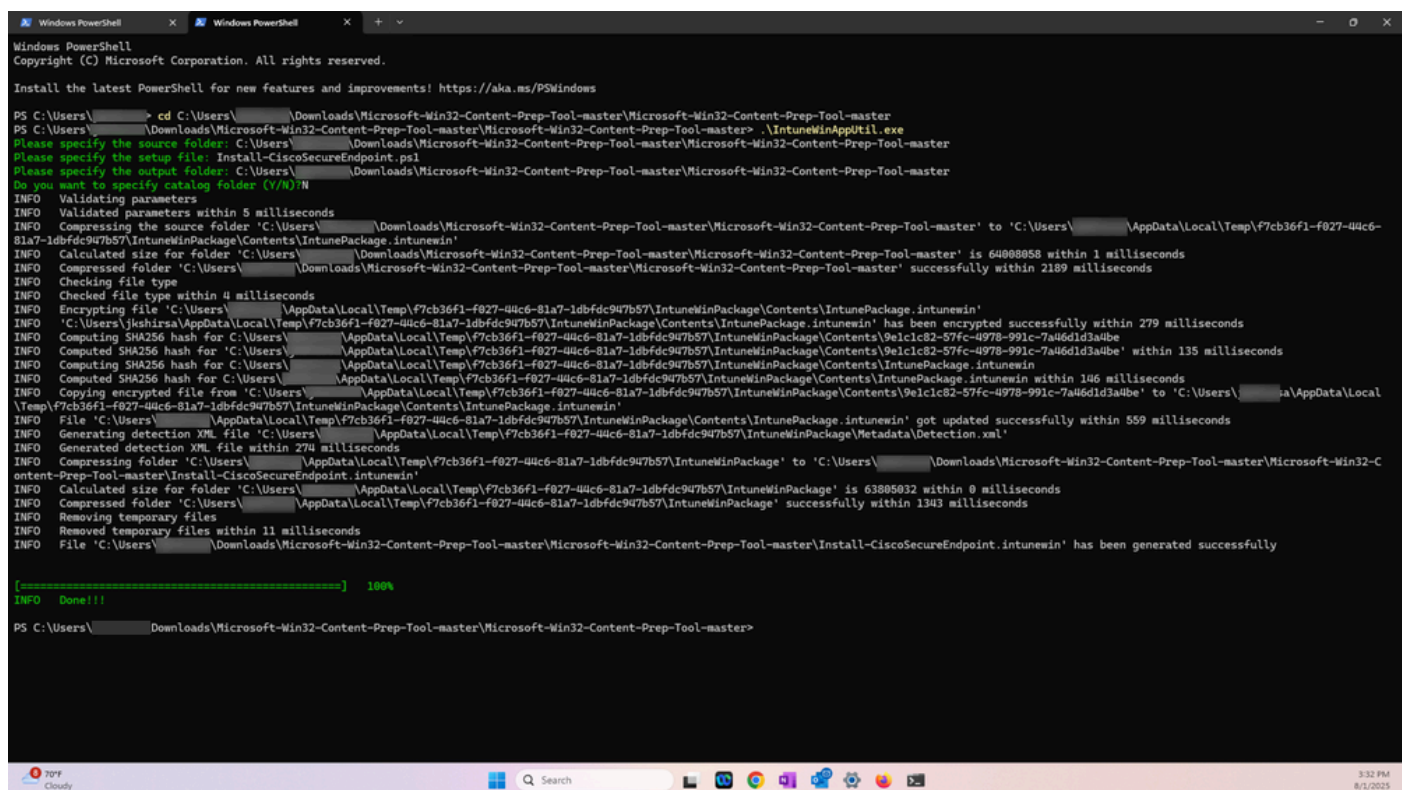
Etapa 2. Prepare o arquivo do Intune usando a Ferramenta de Preparação de Conteúdo Win32.

A Ferramenta de Preparação de Conteúdo Win32 é um utilitário fornecido pelo Microsoft Intune para ajudar os administradores de TI a prepararem aplicativos Win32 (ou seja, aplicativos

tradicionais da área de trabalho do Windows) para implantação por meio do Microsoft Intune. A ferramenta converte instaladores de aplicativos Win32 (como .exe, .msi e arquivos relacionados) em um formato de arquivo .intunewin, que é necessário para implantar esses aplicativos via Intune.

Para preparar o arquivo do Intune, siga estas etapas:

- Baixe a ferramenta Win32 Content Prep do Github. Download: <https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool>
- Execute o IntuneWinAppUtil.exe
- Na próxima etapa, altere o diretório para a pasta que contém o arquivo executável do Cisco Secure Endpoint que foi baixado na etapa 1 e o script de instalação do powershell (Install-CiscoSecureEndpoint.ps1)
- Em seguida, especifique o nome do arquivo de script para o arquivo de configuração: Instalação-CiscoSecureEndpoint.ps1
- Na próxima etapa, especifique a pasta onde o arquivo Intunewin deve ser gerado
- Digite N, quando solicitado a especificar o catálogo
- O arquivo Intunewin é gerado como mostrado na captura de tela:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\...> cd C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master
PS C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master> .\IntuneWinAppUtil.exe
Please specify the source folder: C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master
Please specify the setup file: Install-CiscoSecureEndpoint.ps1
Please specify the output folder: C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master
Do you want to specify catalog folder (Y/N) N
INFO Validating parameters
INFO Validating parameters within 5 milliseconds
INFO Compressing the source folder 'C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' to 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO Calculated size for folder 'C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' is 64888858 within 1 milliseconds
INFO Compressed folder 'C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' successfully within 2189 milliseconds
INFO Checking file type
INFO Checked file type within 4 milliseconds
INFO Copying encrypted file from 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO File 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 279 milliseconds
INFO Computing SHA256 hash for 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\9e1c1c82-57fc-4978-991c-7a46d1d3a4be' within 135 milliseconds
INFO Computing SHA256 hash for 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' within 146 milliseconds
INFO Computed SHA256 hash for 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' within 146 milliseconds
INFO Copying encrypted file from 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\9e1c1c82-57fc-4978-991c-7a46d1d3a4be' to 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO File 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 559 milliseconds
INFO Generating detection XML file 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Metadata\Detection.xml'
INFO Generated detection XML file within 274 milliseconds
INFO Compressing folder 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' to 'C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master\Install-CiscoSecureEndpoint.intunewin'
INFO Calculated size for folder 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' is 63805832 within 0 milliseconds
INFO Compressed folder 'C:\Users\...AppData\Local\Temp\7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' successfully within 1343 milliseconds
INFO Removing temporary files
INFO Removed temporary files within 11 milliseconds
INFO File 'C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master\Install-CiscoSecureEndpoint.intunewin' has been generated successfully

[=====] 100%
INFO Done!!!

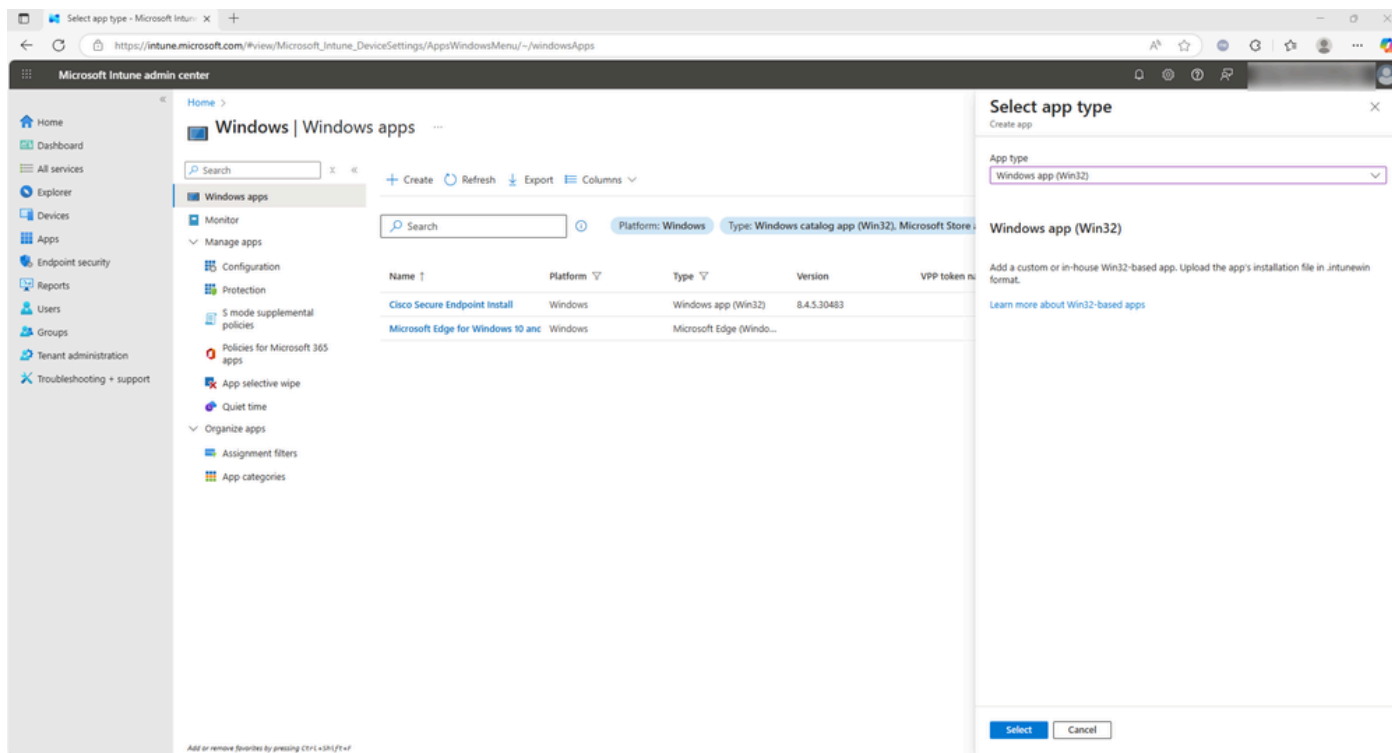
PS C:\Users\...Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master>
```

Etapa 3. Carregue o Arquivo IntuneWin do Ponto de Extremidade Seguro para o Centro de Administração do Microsoft Intune.

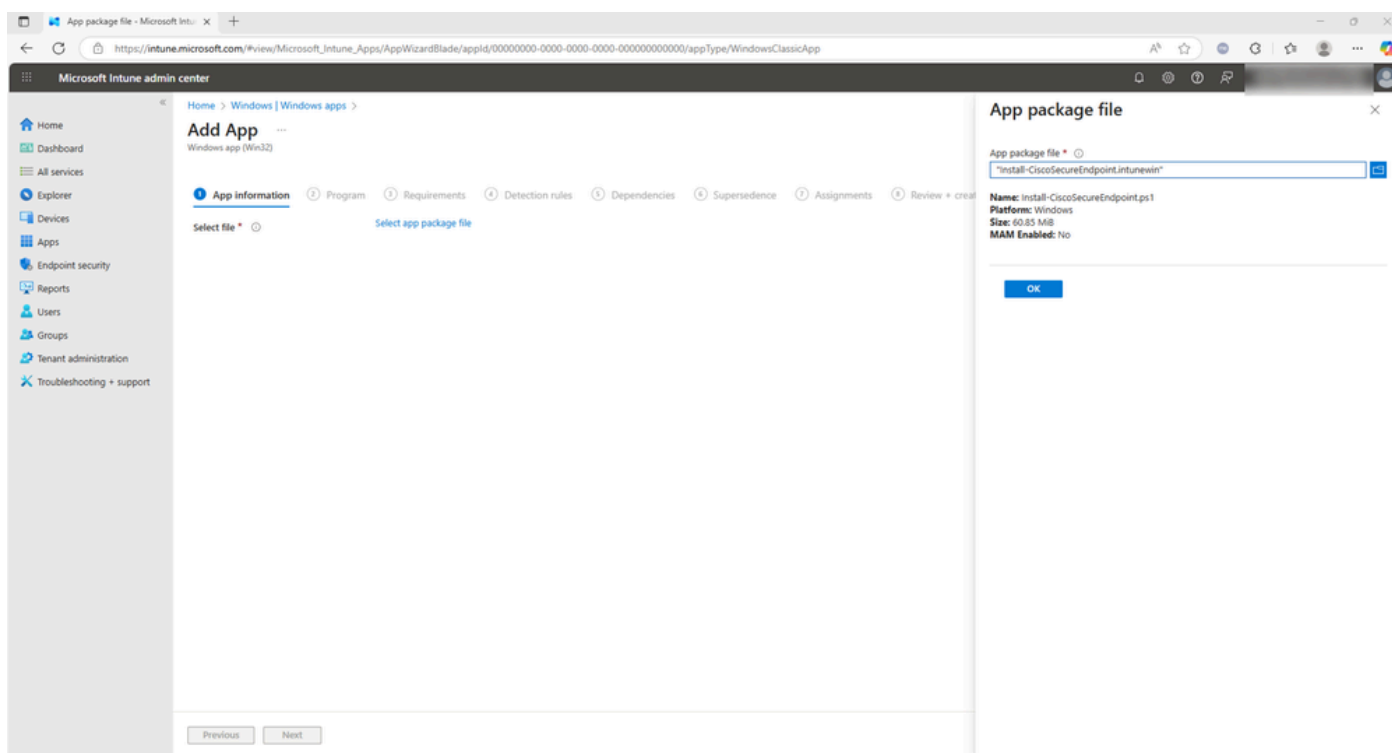
Execute as seguintes etapas:

- Faça login no Centro de Administração do Microsoft Intune
- Navegue para os Aplicativos do Windows no Centro de Administração do Microsoft Intune e selecione Tipo de Aplicativo - Win32 e selecione

Essas duas ações são demonstradas na captura de tela:



- Na próxima etapa, carregue o arquivo Secure Endpoint Intunewin criado na etapa 2 e selecione OK



- Depois de selecionar OK, insira as informações como apresentadas na captura de tela. Os campos opcionais podem ser deixados em branco em cada guia. Vá para a próxima etapa selecionando Próximo

- Insira o comando Install como mostrado:

```
%windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -nopprofile -executionpolicy Bypass -file
```

Observe que o código apresentado aqui serve como exemplo e qualquer código pode ser usado como um comando de instalação para este instalador

- Insira Desinstalar como n/a e o tempo de instalação necessário como 60 (opcional). Defina Permitir desinstalação disponível como Não, selecione Instalar comportamento como Sistema e insira todos os detalhes opcionais antes de selecionar Avançar

The screenshot shows the 'Add App' wizard in the Microsoft Intune admin center, specifically the 'Program' tab. The wizard is for a 'Windows app (Win32)'. The 'App information' tab is selected, showing fields for 'Install command', 'Uninstall command', 'Installation time required (mins)', 'Allow available uninstall', 'Install behavior', and 'Device restart behavior'. The 'Install command' is set to '%windir%\SystemNative\WindowsPowerShell\v1.0\powershell.exe -nopprofile -exec...'. The 'Uninstall command' is set to 'n/a'. The 'Installation time required (mins)' is set to '60'. The 'Allow available uninstall' is set to 'No'. The 'Install behavior' is set to 'System'. The 'Device restart behavior' is set to 'App install may force a device restart'. Below these fields, there is a section for 'Specify return codes to indicate post-installation behavior' with a table of return codes and code types.

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

At the bottom of the wizard, there are 'Previous' and 'Next' buttons.

- Na guia Requisitos, marque Não. Permita que este aplicativo seja instalado em todos os sistemas e selecione o sistema operacional mínimo. Preencha e preencha os campos opcionais, se desejar, e selecione Próximo

The screenshot shows the 'Add App' wizard in the Microsoft Intune admin center, specifically the 'Requirements' tab. The wizard is for a 'Windows app (Win32)'. The 'Requirements' tab is selected, showing fields for 'Check operating system architecture', 'Minimum operating system', 'Disk space required (MB)', 'Physical memory required (MB)', 'Minimum number of logical processors required', and 'Minimum CPU speed required (MHz)'. The 'Check operating system architecture' is set to 'No. Allow this app to be installed on all systems.'. The 'Minimum operating system' is set to 'Windows 10 1607'. The 'Disk space required (MB)', 'Physical memory required (MB)', 'Minimum number of logical processors required', and 'Minimum CPU speed required (MHz)' are all empty. Below these fields, there is a section for 'Configure additional requirement rules' with a table of rules.

Type	Path/Script
No requirements are specified.	

At the bottom of the wizard, there are 'Previous' and 'Next' buttons.

- Na guia Regras de detecção, o menu suspenso Formato das regras fornece duas opções: Configure manualmente as regras de detecção e use um script de detecção personalizado. Ambas as opções podem ser selecionadas com base nos requisitos de implantação.
- Ao escolher Configurar manualmente as regras de detecção, você pode definir um tipo de regra, como MSI, Arquivo ou Registro, para detectar a presença do aplicativo. Neste

documento, a opção alternativa, Usar um script de detecção personalizado, foi selecionada.

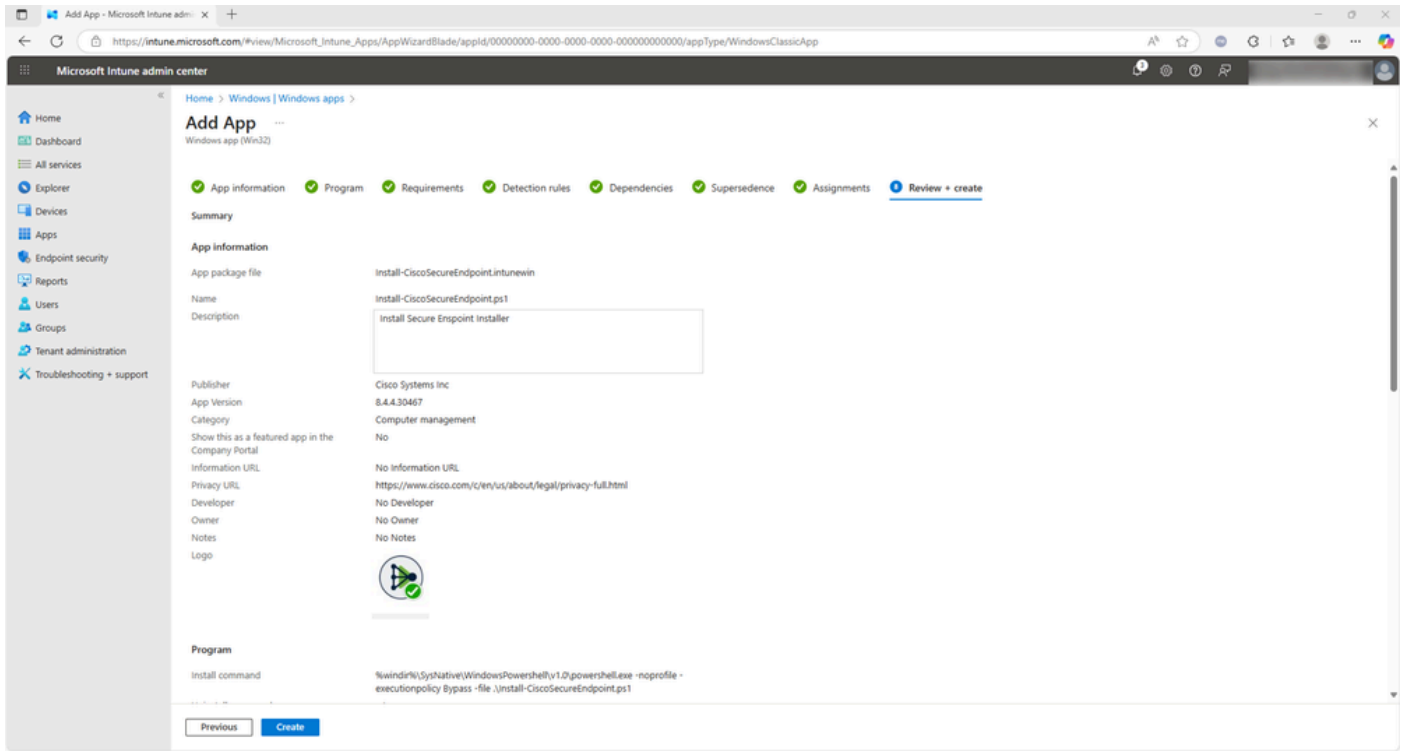
- Um script do PowerShell chamado Confirm-CSEInstall.ps1 é usado para verificar a instalação bem-sucedida do Cisco Secure Endpoint. Ele está listado na parte inferior deste documento.

The screenshot shows the 'Add App' wizard in the Microsoft Intune admin center, specifically the 'Detection rules' step. The wizard is titled 'Add App' and 'Windows app (Win32)'. The 'Detection rules' step is highlighted with a green checkmark. The 'Rules format' dropdown is set to 'Use a custom detection script'. The 'Script file' dropdown is set to 'Confirm-CSEInstall.ps1'. The 'Script content' text area contains the following PowerShell script:

```
[CmdletBinding()]  
param ()  
  
$version = "2.4.4.30467"  
  
<#
```

At the bottom of the wizard, there are two toggle switches: 'Run script as 32-bit process on 64-bit clients' (set to 'No') and 'Enforce script signature check and run script silently' (set to 'No'). At the very bottom, there are 'Previous' and 'Next' buttons.

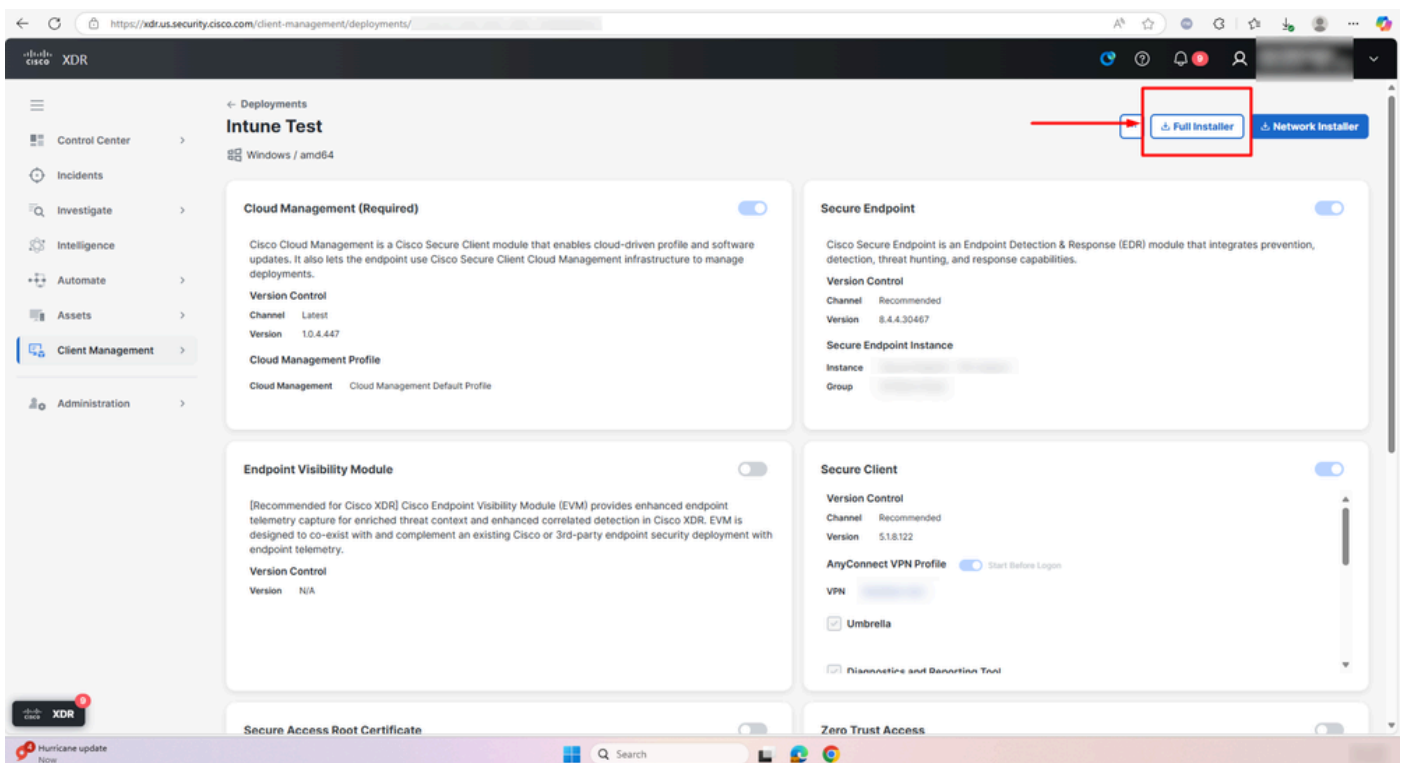
- Selecione Avançar para continuar. Note: Um script de detecção personalizado pode ser criado especificamente para este processo de implantação para se adequar ao seu ambiente e aos critérios de detecção.
- As próximas guias são opcionais. Nenhuma dependência precisa ser configurada, atribua o aplicativo ao grupo necessário e selecione Revisar + criar



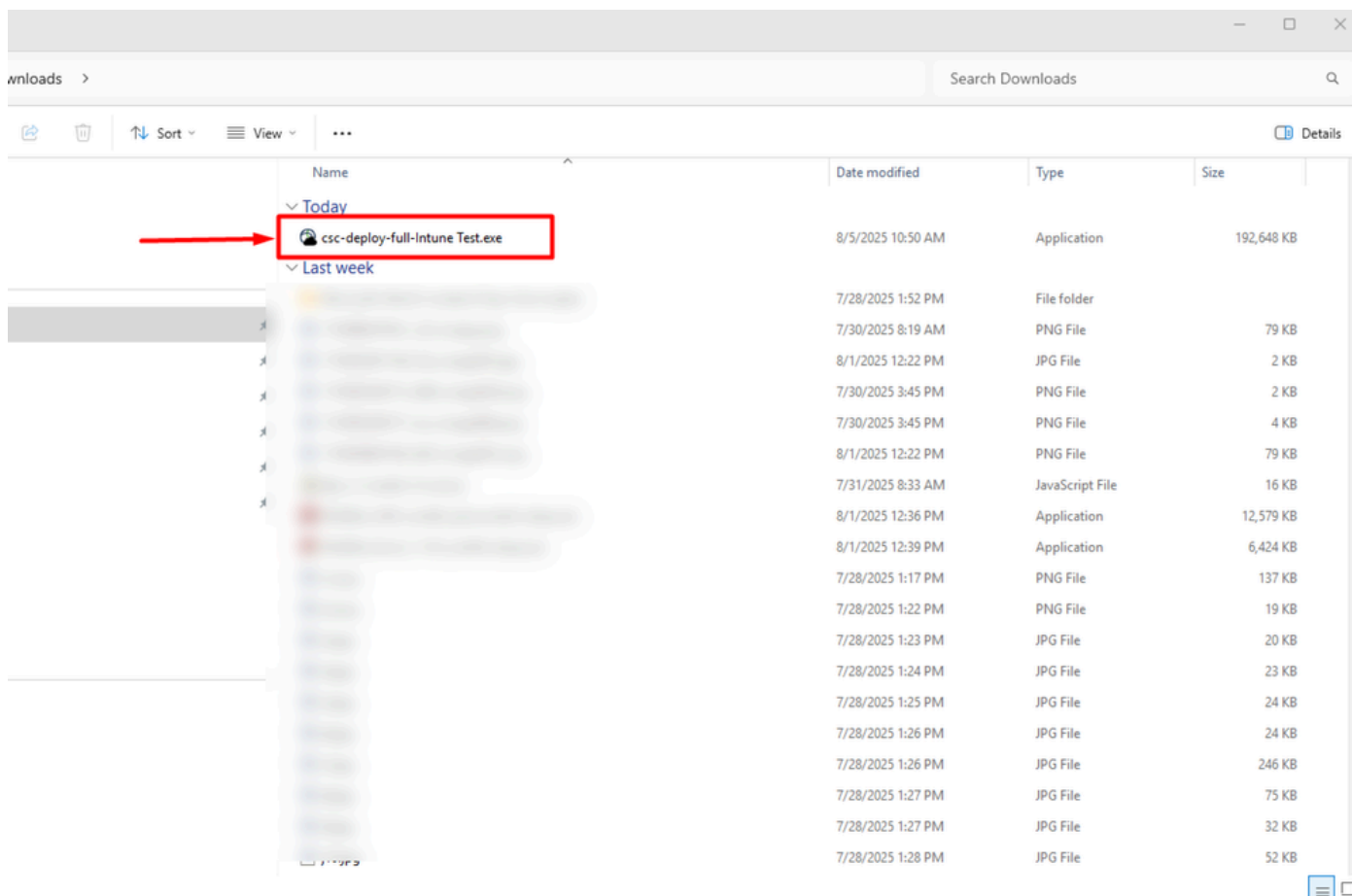
Implantação segura de cliente

Etapa 1. Faça o download da implantação completa do Cisco Secure Client

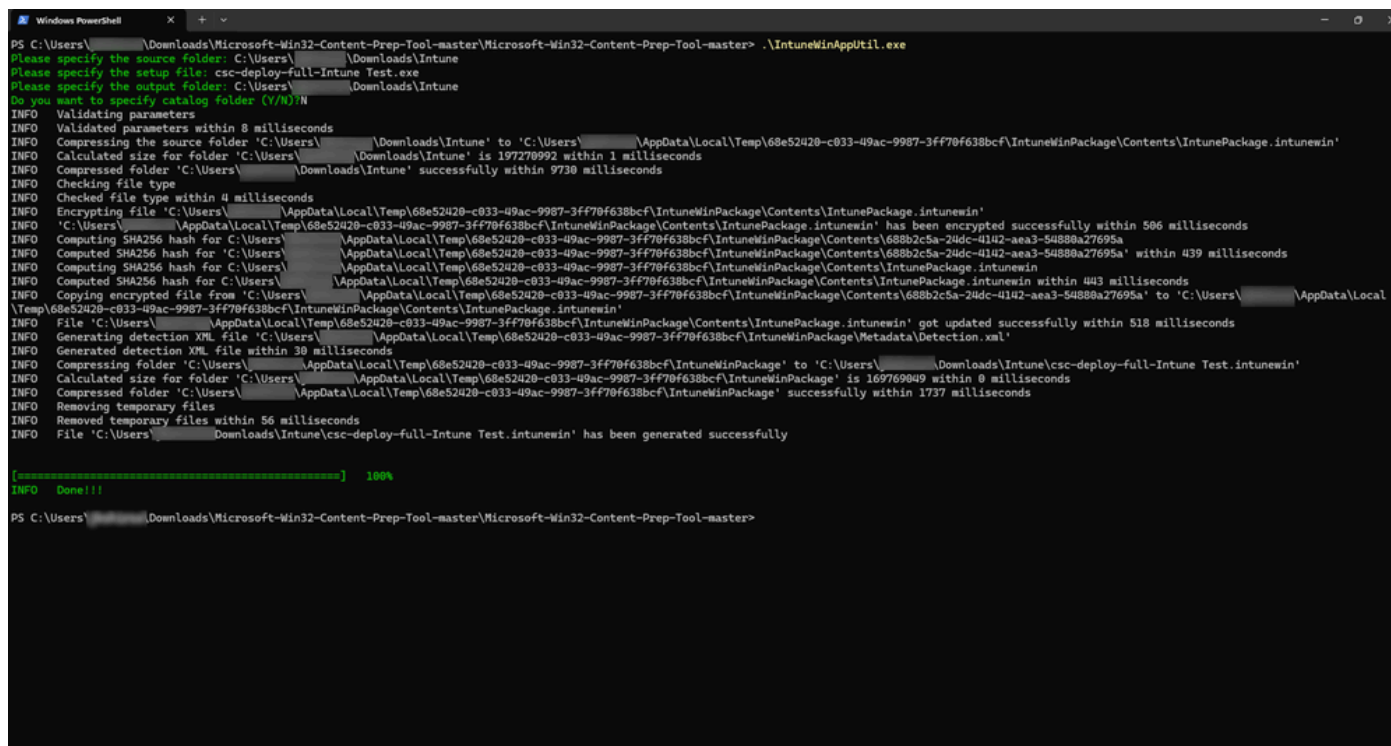
- Faça login no console XDR ou Secure Client Cloud Management, dependendo da região: <https://apps.security.cisco.com/overview>
- Crie uma nova implantação e selecione Full Installer ou Network Installer, dependendo do tipo de implantação



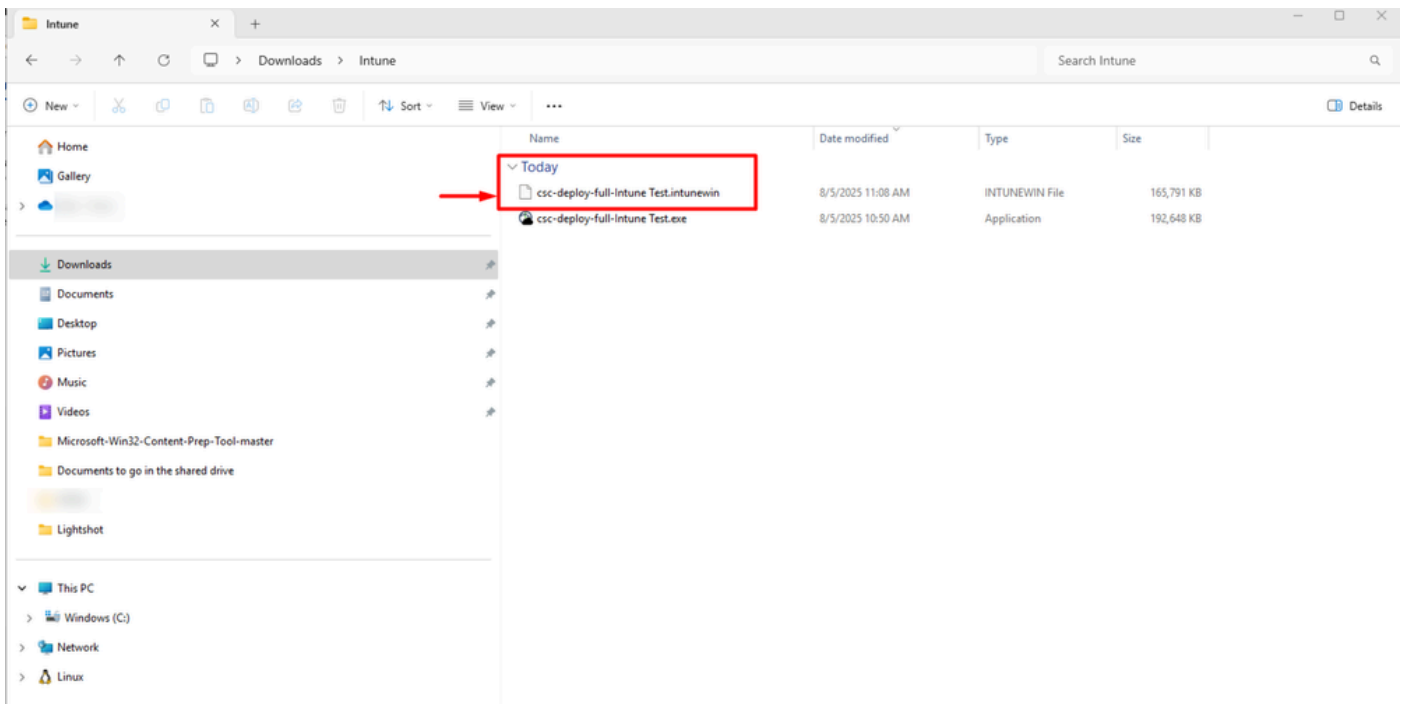
- Um csc-deploy-full-Intune Test.exe é baixado como mostrado na captura de tela.



Etapa 2. Prepare o arquivo do Intune seguindo o mesmo procedimento na etapa 2. Isso cria o arquivo csc-deploy-full-Intune Test.intunewin.



- As etapas acima resultam na criação de um arquivo csc-deploy-full-Intune Test.intunewin, como mostrado na captura de tela.



Etapas 3. Carregue o arquivo csc-deploy-full-intune Test.intunewin da parte 1 para o Centro de Administração do Microsoft Intune conforme as etapas mostradas acima.

Isso conclui o processo para implantar o Cisco Secure Endpoint usando o Intune.

Script Install-CiscoSecureEndpoint.ps1

```
[CmdletBinding()]
param ()

$cse_exe =

$version =

if ($PSCommandPath -eq $null) {
    function GetPSCommandPath() {
        return $MyInvocation.PSCommandPath;
    }
    $PSCommandPath = GetPSCommandPath
}
```

```

$script = [pscustomobject]@{
    "Path" = Split-Path $PSCommandPath -Parent
    "Name" = Split-Path $PSCommandPath -Leaf
}

Set-Location -Path $script.Path

$cse_installer = [IO.Path]::Combine($script.Path, $cse_exe)
$csc_installer_args = "/R /S"

<#
    Cannot use -wait for 'Cisco Secure Endpoint' and therefore cannot get the exit code to return.
    Using -wait, returns varied results, instead use Get-Process and while loop to wait for installation
#>
$install = Start-Process -WorkingDirectory "$($script.Path)" -FilePath "${cse_installer}" -ArgumentList $csc_installer_args

while (Get-Process "$($cse_exe -replace '.exe', '')" -ErrorAction SilentlyContinue)
{
    Start-Sleep -Seconds 10
}

```

Script Confirm-CSEInstall.ps1

```

[CmdletBinding()]
param ()

$version =

<#
https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-win32-add#step-4-detection-rules
    The app gets detected when the script both returns a 0 value exit code and writes a string value to the standard error (STDERR) stream.

    The Intune agent checks the results from the script. It reads the values written by the script to the standard error (STDERR) stream, and the exit code. If the script exits with a nonzero value, the application detection status isn't installed. If the exit code is zero and STDOUT has data, the detection status is installed.
#>

$cse = Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\*, HKLM:\SOFTWARE\Wow6432bit\Uninstall\*
if ($cse | Where-Object { [System.Version] $_.DisplayVersion -ge [System.Version] "${version}" })
{
    Write-Host "Installed"
    exit 0
}

exit 1

```


Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.